(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 September 2005 (15.09.2005)

PCT

(10) International Publication Number
WO 2005/084252 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/006279

(22) International Filing Date: 1 March 2005 (01.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/549,223 2 March 2004 (02.03.2004) US
11/067,859 28 February 2005 (28.02.2005) US

(71) Applicant *(for all designated States except US)*: MACROVISION CORPORATION [US/US]; 2830 De La Cruz Boulevard, Santa Clara, CA 95050 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: BASCHE, Todd [US/US]; 1060 Estrellita Way, Los Altos, CA 94022 (US). SRINIVASAN, Usha [US/US]; 1083 Bluebird Avenue, Santa Clara, CA 95051 (US). PATTERSON, James [US/US]; 2295 Broadway, #4, San Francisco, CA 94115 (US). PANCHOLY, Mitesh [US/US]; 421 Ellis Street, #401, San Francisco, CA 94102 (US).

(74) Agent: SALTER, James, H.; Macrovision Corporation, 2830 De La Cruz Boulevard, Santa Clara, CA 95050 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM, METHOD AND CLIENT USER INTERFACE FOR A COPY PROTECTION SERVICE

(57) Abstract: A system, method and client user interface for a copy protection service employs software agents masquerading as nodes in decentralized networks for monitoring and interdicting file sharing activities of protected files in the networks. A control center communicates with the software agents and subscriber client computers through user interfaces, so as to provide monitoring information to users of the client computers and control the monitoring and interdiction of protected files according to instructions received from the client computers. A one-click method for requesting protection of a file, providing the terms of such protection, and updating billing information for the user is implemented through the user interface to simplify user interaction with the copy protection service.

WO 2005/084252 A2

BEST AVAILABLE COPY

SYSTEM, METHOD AND CLIENT USER INTERFACE FOR A COPY PROTECTION SERVICE

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. provisional application serial no. 60/549,223 filed March 2, 2004, which is incorporated herein by reference.

FIELD OF THE INVENTION

[0002] The present invention generally relates to the interdiction of unauthorized copying in decentralized networks and in particular, to a system, method and client user interface for a copy protection service.

BACKGROUND OF THE INVENTION

[0003] Unauthorized copying in decentralized networks using peer-to-peer (P2P) file sharing has become a major concern to owners of copyrighted material. Unlike a centralized network, decentralization makes it commercially impractical to pursue all copyright violators in court. This is because decentralization requires filing lawsuits against virtually millions of client computer operators instead of only one party operating a central computer.

[0004] Accordingly, copyright owners seek other methods for protecting their copyrighted material, such as blocking, diverting or otherwise impairing the unauthorized distribution of their copyrighted works on a publicly accessible decentralized or P2P file trading network. In order to preserve the legitimate expectations and rights of users of such a network, however, it is desirable that copyright owners do not alter, delete, or otherwise impair the integrity of any computer file or data lawfully residing on the computer of a file trader.

[0005] U.S. Pat. No. 6,732,180 describes one method of interdicting unauthorized copying in a decentralized network using decoy files. In the method described, the network is scanned for media to be protected. When such media is found, decoy files are distributed through controlled nodes in the network so as to reduce the likelihood of a successful download. The number of controlled nodes in this case is determined so as to satisfy a specified effective decoy ratio related to the number of nodes offering decoy versions of the media and the total number of nodes offering real versions of the media.

[0006] The cost and advanced technology to implement and maintain such a system to interdict unauthorized copying of protected files may be prohibitive, however, for many content owners. To satisfy the needs of these and other owners of the content of files, a copy protection services industry has developed in recent years. Interfaces to and information provided by such service companies, however, are generally crude and/or difficult to customize to the individual needs and/or preferences of content owners. This is especially apparent where a content owner may desire to define different levels of protection among its owned content, in order to balance the cost of protection against any financial benefit of such protection.

OBJECTS AND SUMMARY OF THE INVENTION

[0007] Accordingly, it is an object of one or more aspects of the present invention to provide a system, method and client user interface for a copy protection service that provides user selectable monitoring information formats for protected files.

[0008] Another object is to provide such a system, method and client user interface that provides an alert mechanism for automatically informing a user

when a protected file has reached a user specified threshold level in a decentralized network.

[0009] Another object is to provide such a system, method and client user interface that provides user selectable interdiction levels for protected files in a decentralized network.

[0010] Still another object is to provide such a system, method and client user interface that is easy for a user to interface with for specifying such monitoring and interdiction requirements and levels.

[0011] Yet another object is to provide such a system, method and client user interface that automatically adjusts billing information for a user as the user modifies interdiction levels for protected files.

[0012] These and additional objects are accomplished by the various aspects of the present invention, wherein briefly stated, one aspect is a system for providing a copy protection service, comprising: a plurality of software agents masquerading as nodes in a decentralized network for monitoring and interdicting file sharing activities of a protected file; and a control center configured to communicate with the plurality of software agents and a client computer, so as to provide information of such monitoring to the client computer and control such monitoring and interdicting according to instructions received from the client computer.

[0013] Another aspect is a method for providing a copy protection service, comprising: receiving file information for one or more protected files in one or more decentralized networks from a plurality of software agents masquerading as nodes in the one or more decentralized networks; providing the file information to one or more client computers respectively associated with individual of the one or more protected files; receiving interdiction instructions from the one or more client computers; and commanding the plurality of software

agents to interdict file sharing activities in the one or more decentralized networks for the one or more protected files according to the interdiction instructions.

[0014] Another aspect is a one-click method for providing a copy protection service, comprising: receiving a protection command associated with a protected file from a client computer; updating billing information associated with the client computer to reflect the protection command; and interdicting file sharing activities for the protected file in a decentralized network according to the protection command.

[0015] Still another aspect is a user interface method associated with a copy protection service, comprising: displaying information of a protected file in a decentralized network on a display screen of a client computer; and displaying a user selectable protection option on the display screen so that upon selection of the user selectable protection option and specification of interdiction terms by a user of the client computer, a protection request to interdict file sharing activity of the protected file in the decentralized network is transmitted to a control center providing a copy protection service.

[0016] Additional objects, features and advantages of the various aspects of the present invention will become apparent from the following description of its preferred embodiment, which description should be taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] **FIG. 1** illustrates a block diagram of a system for providing copy protection services, utilizing aspects of the present invention.

[0018] **FIG. 2** illustrates a block diagram of a control center in a system for providing copy protection services, utilizing aspects of the present invention.

[0019] **FIG. 3** illustrates a Home-page screen-shot generated through a user interface, utilizing aspects of the present invention.

[0020] **FIG. 4** illustrates a "WatchLists" sub-page screen-shot generated through a user interface, utilizing aspects of the present invention.

[0021] **FIG. 5** illustrates an "Alerts" sub-page screen-shot generated through a user interface, utilizing aspects of the present invention.

[0022] **FIG. 6** illustrates a "Pop-Up" screen-shot generated through a user interface, utilizing aspects of the present invention.

[0023] **FIG. 7** illustrates a "Reports" sub-page screen-shot generated through a user interface, utilizing aspects of the present invention.

[0024] **FIG. 8** illustrates a "Search" sub-page screen-shot generated through a user interface, utilizing aspects of the present invention.

[0025] **FIG. 9** illustrates a flow diagram of a "One-Click" method for providing a copy protection service, utilizing aspects of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0026] **FIG. 1** illustrates, as an example, a block diagram of a System providing a copy protection service for interdiction of unauthorized copying of files residing on Nodes (such as nodes N1~N15) of a Decentralized Network **101**. The Decentralized Network **101** is a peer-to-peer file sharing network configured such as any of those being used to share files of copyrighted material through free downloading of copies without paying appropriate compensation to their respective copyright owners.

[0027] In addition to copy protection, the System also provides a web-based reporting and analysis application that gathers and synthesizes large amounts of piracy-related data for catalog titles on various filing sharing networks (such as the Decentralized Network 101 as well as others). Subscribers can thus monitor file-sharing activity related to specific titles in their catalog, generate reports on metrics such as supply, demand and availability for a title on any network and further refine charts displayed to the User by geography (e.g., DMA, country, etc.) and/or domain.

[0028] Although in the following description, the files to be protected are assumed to be music files, the copy protection service can be used to protect any type of file or object as those terms are conventionally understood, such as or as well as, a document, message, computer program, data, all forms of media (such as audio, video, animation, and images), and any other content or information protected under copyright or any other intellectual property law that is capable of being communicated between two nodes of a network.

[0029] In a decentralized network, there is no central authority or managing entity. Each node of the decentralized network makes decisions autonomously to connect, disconnect, and share information with other nodes in the decentralized network according to a predetermined protocol established by the creators of the decentralized network. Files are stored in the nodes of the decentralized network and propagated throughout the decentralized network via inter-nodal exchange. Users of the nodes search the decentralized network using search queries at their respective nodes for specific files and then select a host node from the search results to download or stream the content from.

[0030] Components of the System include a Control Center 102, a plurality of Software Agents (such as agents SA1~SA3) masquerading as nodes of the Decentralized Network 101 by following all the traditions and policies of the Decentralized Network 101 so that the Software Agents are virtually

indistinguishable as infiltrators, and Client Application Software residing on Client Computers (such as clients **104~106**) operated by Users authorized to access the System as or by Subscribers of the copy protection service.

[0031] The Software Agents are uniformly distributed throughout the Decentralized Network **101** to perform instrumentation and/or interdiction functions. The Software Agents are implemented as software or agents residing on one or more computers that communicate with Nodes in the Decentralized Network **101** through individually assigned ports of the computers on which they reside. IP addresses for the ports may vary with time or in some other manner so that detection of the Software Agents as unauthorized masqueraders of nodes in the Decentralized Network **101** is made difficult.

[0032] Similar software agents are placed in other decentralized networks for instrumentation and interdiction purposes. Like the Software Agents in the Decentralized Network **101**, these other software agents are also controlled by and communicate with the Control Center **102**.

[0033] **FIG. 2** illustrates, as an example, a block diagram of the Control Center **102** which is preferably implemented by various software modules running on one or more computers. A User Interface Manager **201** controls access to the copy protection service by Users of Client Computers (such as **104~106**) through a conventional log-on procedure on a Website hosted by the Control Center **102**, and manages the flow of information from and to the Client Computers in cooperation with client application software residing on the Client Computers. The client application software manages the display of information through a Client User Interface running as an application launched in Web Browsers on the Client Computers.

[0034] A number of software modules support the User Interface Manager **201** in its information exchanges with the client application software,

and their display through the Client User Interface. Among these supporting software modules are a Piracy Index module **211**, a WatchLists module **212**, an Alerts module **213**, a Reports module **214**, a Catalogs module **215**, and a Search Engine module **216**, whose use and operations will be explained below.

[0035] Database **202** stores Subscriber information including content owned and content paid to be copy protected by the Subscriber, and the level (i.e., Platinum, Gold or Silver) and duration of any such copy protection. Catalog data comprising for each music file, the artist, the album and the corresponding track title is included in such Subscriber information. For accurate identification of copies of the music files on decentralized networks being monitored by the System, metadata and audio content for each such title are also included.

[0036] A Billing System **230** keeps track of charges and invoices the Subscribers according to information stored in the Database **202**.

[0037] An Interdiction System **230** performs copy protection activities by sending instructions to the Software Agents (such as agents SA1~SA3) through a private network specifying actions to be taken when the Software Agents receive search results or search strings identifying files that are to be protected by the copy protection service according to information stored in a database ("DB") **231** in the Interdiction System **230**. Additional details of such an interdiction system are provided, for example, in commonly-owned U.S. Applic. Ser. No. 10/803,784 filed March 18, 2004, which is incorporated herein in its entirety by this reference.

[0038] An Instrumentation System **240** estimates various characteristics of the Decentralized Network **101**, such as: the size, growth rate, and growth acceleration of the Decentralized Network **101**; the number of instances, the rate of propagation, and the acceleration of propagation of a file in the Decentralized Network **101**; and the search and download activities, in the aggregate and for

particular files, in the Decentralized Network **101**. Additional details of such an instrumentation system are provided, for example, in commonly-owned U.S. Applic. Ser. No. 10/818,674 filed April 6, 2004, which is incorporated herein in its entirety by this reference.

[0039] **FIG. 3** illustrates, as an example, a home-page (My Hawkeye) screen-shot generated through the Client User Interface. The lay-out of the dashboard or home-page is customizable by the Subscriber's authorized User running the application, and provides a portal view to display a combination of supported components. It allows the User easy access to features of interest on one page, and reduces the need to navigate multiple screens of the Console. All components of this view are a replication of functionalities fully implemented in other areas of the Console.

[0040] A Tab Line (or Navigation Menu) **301** facilitates User selection of predefined pages to be displayed such as a WatchLists-page through a WatchLists-tab, an Alerts-page through an Alerts-tab, a Reports-page through a Reports-tab, a Search-page through a Search-tab, a Catalog-page through a Catalog-tab, and a Feedback-page through a Feedback-tab. Also provided on the Tab Line **301** are tabs for conventional Help and Logout functions.

[0041] A Piracy Index line **302** indicates the number of illegal files found in the Decentralized Network **101** for a catalog of music files that is selected using a drop-down box or pull-down menu **311**. The catalog in this case may be the Subscriber's catalog of music files (My Catalog) or a catalog of music files for the entire music industry (Industry).

[0042] In addition to the total number of illegal files indicated in area **313**, the change in the number of illegal files found over a specified period of time is indicated in area **314** with increase or decrease respectively indicated by lighting either an up or down arrow preceding the area **314**. The period of time is

specified in this case using drop-down box **312**, providing a choice of time periods such as over the last hour, the last day, the last week, the last month, etc.

[0043] Determination of the number of illegal files in the Decentralized Network **101** and the change in such illegal files is performed by the Instrumentation System **240**. The Piracy Index module **211** communicates the information provided in drop-down boxes **311** and **312** to the Instrumentation System **240**, and communicates the results generated by the Instrumentation System **240** to the User Interface Manager **201** for display in areas **313** and **314**.

[0044] A WatchList area **303** includes information for a selected WatchList of music files. This area provides a quick view of the extent of illegal file activity for the music files in the WatchList, and the effectiveness of any copy protection activities. Additional details on this area are described in reference to **FIG. 4**.

[0045] An area **304** displays graphs according to attributes designated in corresponding drop-down boxes. This area provides a quick visual view of the designated attributes using information provided by the Instrumentation System **240**. In particular, attributes such as supply, demand, availability, effectiveness indices, and various growth and acceleration rates can be viewed over a combination of two independent variables such as: type of file sharing network, geography (DMA, country, etc.), organization (or domain), and time. As an example, the User can specify a chart or graph on the penetration of the "Ray of Light" track by Madonna by network in the Los Angeles area (DMA) or view the rate of change of demand for Sheryl Crow's "Leaving Las Vegas" by network over time.

[0046] For every chart (or graph) the User has the option to save the chart graphics onto his or her desktop in a format (e.g., SVG, EPS) that permits lossless

scaling and object decomposition in the destination environment. This allows the User to use the chart in reports and presentations.

[0047] Additionally, the User can also export the data associated with the chart to his or her desktop in a format (e.g., CSV) that permits pasting into Microsoft Excel.

[0048] **FIG. 4** illustrates, as an example, a WatchLists-page screen-shot generated by the Client User Interface upon User selection of the WatchLists tab 401.

[0049] There are two basic types of WatchLists. The first type is System-Defined WatchLists. These lists are "prefabricated" and the User has no choice in what works are included in the list, or what metrics are monitored and presented for display. In general, the System-Defined WatchLists provide a useful snapshot of industry-wide data and trends in supply and demand for protected works on the monitored file-sharing networks. These lists are automatically generated by the System based on statistical analysis of data gathered for the entire catalog. Examples of System-Defined WatchLists are: Top 10 Artists by Demand, and Top 10 Albums by Supply.

[0050] The second type of WatchLists is User-Defined WatchLists. These lists are created by the User. This type of WatchLists is provided as a convenience to the User so that the User can keep track of a subset of works in a catalog deemed of interest to the User. It also enables keeping track of different lists of works separately for the purpose of monitoring different metrics for different activities. The User can create these WatchLists and add or remove tracks to and from the lists at will. The contents (works) of the lists are static and won't change unless the User decides to do so. Examples of User-Defined WatchLists are: My Favorite Soul Songs, and Madonna's hit singles.

[0051] The User selects the WatchList to be viewed through drop-down box 402. The User may also select the time period (e.g., last week, last month, etc.) to be used for calculating any displayed metrics through drop-down box 403. An Alerts column 411 indicates whether an alert has been set against the corresponding title (or track). An Artist column 412, Album column 413, and Track column 414 respectively display artist, album, and track information for each music file in the selected WatchList.

[0052] A Penetration column 415, Supply Index column 416, Demand Index Column 417, and Effectiveness column 418 respectively display information of consolidated metrics for the penetration, supply, demand, and effectiveness of protection (if protected) for each music file in the selected WatchList. Although metrics are computed on a per network basis by the Instrumentation System 240, they are consolidated for all supported networks when reported in the WatchLists.

[0053] A Protection column 419 displays a protect button for each music file in the selected WatchList. If the music file is currently protected, the level of protection (e.g., Platinum, Gold, or Silver) is displayed in lettering on its corresponding protect button. On the other hand, if the music file is currently unprotected, the word "Protect" is displayed on its corresponding protect button. When the User clicks one of the protect buttons, a Pop-Up window appears (such as 601 of FIG. 6) and protection for the corresponding music file can be initiated or its level and/or duration modified.

[0054] Export Options 421 are provided so that information in the WatchList may be exported to other applications such as Excel, or as an XML or CSV file.

[0055] FIG. 5 illustrates, as an example, an Alerts-page screen-shot generated by the Client User Interface. This page facilitates event-triggered email

alerts that can be defined by the User. An event can be, for example, a first appearance of a protected title on a monitored network or the value of a metric crossing a User-Defined threshold value. These alerts allow the User to closely monitor supply, demand and availability of titles and use the trend and event information for decision-making.

[0056] Drop-Down boxes **511, 512, 514** and type-in box **513** facilitate definition of the event by the User. Drop-Down box allows specification of an email address that alerts are to be sent to. Selectable email addresses in this case specified by the Subscriber, and stored in Subscriber profile information in the Database **202**. Creation or updating of an event is triggered by the User clicking the Create button **531** or the Update button **532**, as the case may be. Alerts can be deleted by clicking the appropriate check in the Delete column **542**.

[0057] **FIG. 6** illustrates, as an example, a protection Pop-Up **601** generated by the client application software upon detecting a protect button (such as displayed in the Protection column **541**) being clicked by the User. As previously explained, the User can protect a title by clicking its corresponding protect button in the WatchList or Alerts area. The User is provided different options in the Pop-Up **601** that represent different levels of protection such as Platinum **621** for highest level of protection (and highest cost to the Subscriber), Gold **622** for medium level protection, and Silver **623** for lowest level of protection (and lowest cost to the Subscriber). In addition, the User can specify the starting date for such protection in type-in box **611**, and the ending date in type-in box **612**. A second protect button **631** is provided so that the User can confirm that his or her selections have been made and trigger the protection mechanism upon clicking this button.

[0058] This protection enabling procedure allows the User to take interdiction measures with minimal effort. For example, the User may receive an alert informing him or her of the first appearance of a pre-release title. The User

can then immediately issue a protection order for the title to prevent viral propagation of the title on the various file-sharing networks and soon receive metrics that will report the effectiveness of the interdiction campaign, and change in supply, demand, etc.

[0059] **FIG. 7** illustrates, as an example, a reports-page screen-shot generated by the Client User Interface when the User selects the Reports tab **701** in the Navigation Menu. The User selects the artist, album or track in a reports catalog **702** for which reports are to be generated. For the selected title or album, the User selects the chart metric by clicking one of the buttons for Penetration **711**, Supply Index **712**, Demand Index **713**, Effectiveness **714**, or Users **715**; by clicking one of the buttons for Actual Value **721** or Growth **722**; by selecting in Drop-Down boxes **731** and **732** respectively the X-Axis and Y-Axis attributes; by selecting in Drop-Down box **741** the type of chart or graph; and by specifying the time period over which the metrics are to be calculated in Drop-Down box **742**. Once all such selections have been made, then the User may click the Generate Report button **751**, and the generated report is shown in the Report Results area **761**. As previously described, the generated report may then be saved and exported by the User.

[0060] **FIG. 8** illustrates, as an example, a search-page screen-shot generated by the Client User Interface when the User selects the Search tab **801** on the Navigation Menu. The text search feature allows the User to find artists, albums and tracks that contain matching text input by the User in a type-in Artist box **811**, and/or type-in Album box **812**, and/or type-in Track title box **813**. This allows the User to quickly access works for the purpose of monitoring, viewing charts or protecting against piracy. After initiating the search by the User clicking the Search button **821**, the results are displayed in area **802** in an Artist, Album and Track format.

[0061] FIG. 9 illustrates, as an example, a flow diagram of a one-click protection method for protecting user specified content in a system providing a copy protection service. In 901, the clicking by a User of a protect button in a Protection column (such as 541 in FIG. 6) and a Music File (or track) row of a WatchList area is detected through the Client User Interface by, for example, client application software residing on the User's computer.

[0062] In 902, a Pop-Up (such as 601 in FIG. 6) is displayed on the User's display screen through the Client User Interface. The User then inputs the requested information into the Pop-Up, and clicks another protect button (such as 631 in FIG. 6) in the Pop-Up to indicate that the requested information has been provided.

[0063] In 903, the clicking by the User of the second protect button is detected through the Client User Interface by, for example, client application software residing on the User's computer.

[0064] In 904, the User inputs are read by, for example, client application software residing on the User's computer, and passed to the User Interface Manager 201. Examples of such User inputs are the start and end dates for the protection, and the level of protection.

[0065] In 905, the Database 202 is updated with the name of the music file and the User provided information of duration and level of copy protection for billing purposes as used by the Billing System 220, and the database 231 in the Interdiction System 230 is updated with the same name of the music file and the User provided information of duration and level of copy protection for copy protection purposes as used by the Interdiction System 230.

[0066] Although the various aspects of the present invention have been described with respect to a preferred embodiment, it will be understood that the

invention is entitled to full protection within the full scope of the appended claims.

CLAIMS

What is claimed is:

1. A system for providing a copy protection service, comprising:

a plurality of software agents masquerading as nodes in a decentralized network for monitoring and interdicting file sharing activities of a protected file; and

a control center configured to communicate with the plurality of software agents and a client computer, so as to provide information of such monitoring to the client computer and control such monitoring and interdicting according to instructions received from the client computer.

2. The system according to claim 1, wherein the control center includes an instrumentation system configured to generate the monitoring information by estimating characteristics of the decentralized network.

3. The system according to claim 2, wherein the estimated characteristics include a size of the decentralized network.

4. The system according to claim 3, wherein the estimated characteristics include a growth rate of the decentralized network.

5. The system according to claim 4, wherein the estimated characteristics include a growth acceleration of the decentralized network.

6. The system according to claim 2, wherein the estimated characteristics include a number of instances of the protected file in the decentralized network.

7. The system according to claim 6, wherein the estimated characteristics include a rate of propagation of the number of instances of the protected file in the decentralized network.

8. The system according to claim 7, wherein the estimated characteristics include an acceleration of propagation of the number of instances of the protected file in the decentralized network.

9. The system according to claim 2, wherein the estimated characteristics include a number of search requests for the protected file over a period of time in the decentralized network.

10. The system according to claim 2, wherein the estimated characteristics include a number of downloads of the protected file over a period of time in the decentralized network.

11. The system according to claim 1, wherein the control center includes an interdiction system configured to control the plurality of software agents so as to perform such interdicting.

12. The system according to claim 1, wherein the client computer is configured with a user interface for communicating with the control center.

13. The system according to claim 12, wherein the monitoring information is presented to a user of the client computer through the user interface.

14. The system according to claim 13, wherein the monitoring information is emailed to a user of the client computer.

15. The system according to claim 14, wherein the monitoring information is emailed to the user according to criteria established by the user.

16. The system according to claim 12, wherein the interdiction instructions are transmitted from the client computer to the control center through the user interface.

17. The system according to claim 16, wherein a protection icon is displayed adjacent the monitoring information by the user interface on a display screen of the client computer, and generation of the interdiction instructions is initiated by the user selecting the protection icon.

18. The system according to claim 17, wherein the user selects the protection icon by clicking on it with a pointing device.

19. The system according to claim 18, wherein a pop-up menu is displayed on the display screen in response to the user clicking on it, and the user specifies duration of interdiction through the pop-up menu.

20. The system according to claim 18, wherein a pop-up menu is displayed on the display screen in response to the user clicking on it, and the user specifies a level of interdiction through the pop-up menu.

21: The system according to claim 20, further comprising a billing system so that the user is appropriately charged for the level of interdiction selected by the user through the pop-up menu.

22. The system according to claim 1, wherein the plurality of software agents masquerade as nodes in a plurality of decentralized networks for monitoring and interdicting file sharing activities of the protected file.

23. The system according to claim 22, wherein the plurality of software agents masquerade as nodes in the plurality of decentralized networks for monitoring and interdicting file sharing activities of a plurality of protected files.

24. The system according to claim 23, wherein the control center is configured to communicate with the plurality of software agents and a plurality of client computers individually associated with one or more of the plurality of protected files so as to provide information of such monitoring to associated ones of the plurality of client computers, and control such interdicting according to instructions received from the plurality of client computers.

25. A method for providing a copy protection service, comprising:

receiving file information for one or more protected files in one or more decentralized networks from a plurality of software agents masquerading as nodes in the one or more decentralized networks;

providing the file information to one or more client computers respectively associated with individual of the one or more protected files;

receiving interdiction instructions from the one or more client computers; and

commanding the plurality of software agents to interdict file sharing activities in the one or more decentralized networks for the one or more protected files according to the interdiction instructions.

26. The method according to claim 25, further comprising: monitoring file sharing activity in the one of more decentralized networks for the one or more protected files to generate the file information.

27. The method according to claim 26, wherein the monitoring of file sharing activity comprises: estimating a number of instances of individual of the one or more protected files in individual of the one or more decentralized networks.

28. The method according to claim 26, wherein the monitoring of file sharing activity comprises: estimating a number of search requests over a period of time for individual of the one or more protected files.

29. The method according to claim 26, wherein the monitoring of file sharing activity comprises: estimating a number of downloads over a period of time for individual of the one or more protected files.

30. The method according to claim 25, wherein the providing of the file information comprises: presenting file information for individual of the one or more protected files to users through user interfaces of the associated one or more client computers.

31. The method according to claim 25, wherein the providing of the file information comprises: emailing file information for individual of the one or more protected files to users of the associated one or more client computers according to pre-established criteria.

32. The method according to claim 25, further comprising: providing a selectable protection option along with the file information to the one or more client computers respectively associated with the individual of the one or more protected files so that users of the one or more client computers initiate generation of the interdiction instructions by selecting the selectable protection option.

33. The method according to claim 32, wherein a pop-up menu is displayed on a display screen of individual of the one or more client computers upon a user selecting the selectable protection option, and the user specifies duration of interdiction through the pop-up menu.

34. The method according to claim 32, wherein a pop-up menu is displayed on a display screen of individual of the one or more client computers upon a user selecting the selectable protection option, and the user specifies a level of interdiction through the pop-up menu.

35. The method according to claim 34, further comprising: charging individual users according to levels of interdiction selected by those users through respectively provided pop-up menus.

36. A one-click method for providing a copy protection service, comprising:

receiving a protection command associated with a protected file from a client computer;

updating billing information associated with the client computer to reflect the protection command; and

interdicting file sharing activities for the protected file in a decentralized network according to the protection command.

37. The method according to claim 36, further comprising: providing information of the protected file in the decentralized network prior to receiving the protection command.

38. The method according to claim 37, wherein the information includes an estimate of a number of instances of the protected file in the decentralized network.

39. The method according to claim 37, wherein the information includes an estimate of a number of search requests over a period of time for the protected file in the decentralized network.

40. The method according to claim 37, wherein the information includes an estimate of a number of downloads over a period of time for the protected file in the file sharing network.

41. The method according to claim 37, wherein the information is provided to a user of the client computer through a user interface residing on the client computer.

42. The method according to claim 37, wherein the information is provided to a user of the client computer by email according to pre-established criteria.

43. The method according to claim 42, wherein the pre-established criteria is specified by the user through the user interface.

44. The method according to claim 37, further comprising: providing a protection option along with the information to the client computer so that the user initiates the protection request by selecting the protection option.

45. The method according to claim 44, wherein the protection option is a clickable button positioned proximate to the information on a display screen of the client computer by the user interface.

46. The method according to claim 45, wherein a pop-up is displayed on the display screen when the user clicks on the clickable button.

47. The method according to claim 46, wherein the pop-up facilitates specification by the user of duration of the interdiction of file sharing activities for the protected file.

48. The method according to claim 46, wherein the pop-up facilitates specification by the user of a level of the interdiction of file sharing activities for the protected file.

49. The method according to claim 36, wherein the billing information includes an identification of the protected file and a level of the interdiction of file sharing activities for the protected file.

50. A user interface method associated with a copy protection service, comprising:

displaying information of a protected file in a decentralized network on a display screen of a client computer; and

displaying a user selectable protection option on the display screen so that upon selection of the user selectable protection option and specification of interdiction terms by a user of the client computer, a protection request to interdict file sharing activity of the protected file in the decentralized network is transmitted to a control center providing a copy protection service.

51. The method according to claim 50, further comprising: receiving the information of the protected file from the control center.

52. The method according to claim 51, wherein the information includes an estimate of a number of instances of the protected file in the decentralized network.

53. The method according to claim 52, wherein the information further includes an estimate of a rate of propagation of the number of instances of the protected file in the decentralized network.

54. The method according to claim 53, wherein the information further includes an estimate of an acceleration of propagation of the number of instances of the protected file in the decentralized network.

55. The method according to claim 50, wherein the information includes an estimate of effectiveness of the interdiction of the file sharing activity of the protected file in the decentralized network.

56. The method according to claim 50, wherein the displaying of information comprises: displaying the information in a user specified graph on the display screen of the client computer.

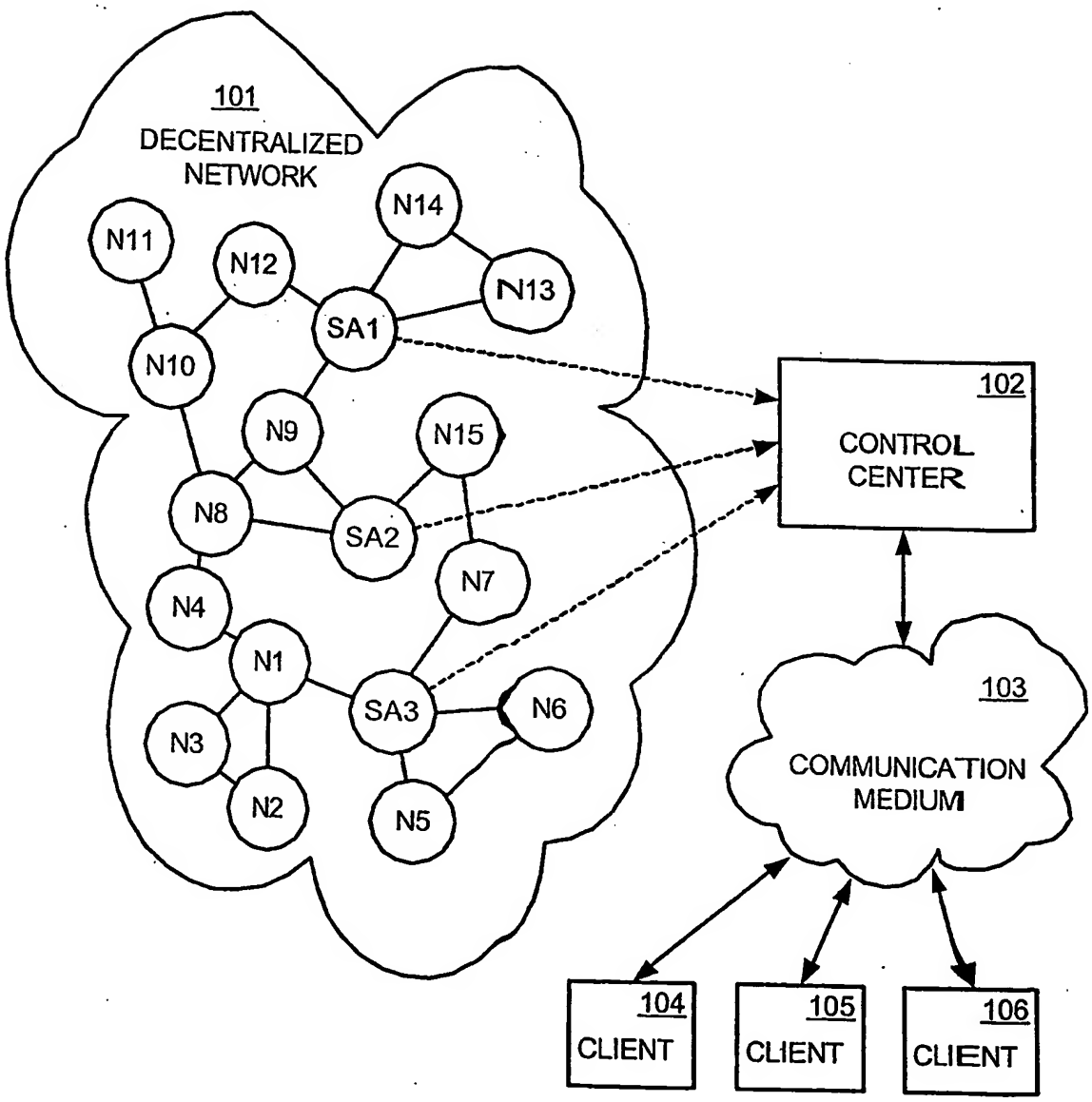
101
DECENTRALIZED NETWORK
N11
N12
N14
N13
SA1
N10
N9
N15
N8
SA2
N7
N4
N1
SA3
N6
N3
N2
N5
102
CONTROL CENTER
103
COMMUNICATION MEDIUM
104
CLIENT
105
CLIENT
106
CLIENT

FIG.1

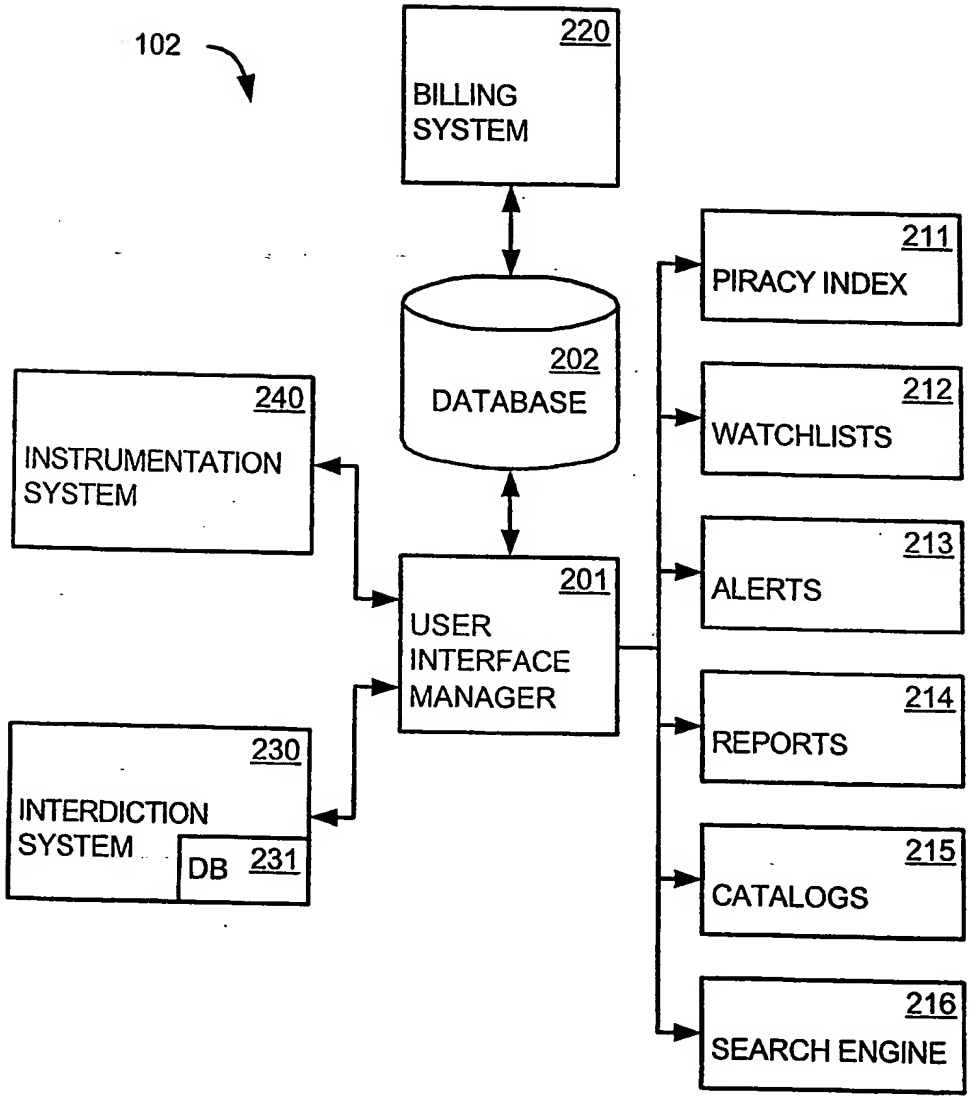
102
220
BILLING SYSTEM
211
PIRACY INDEX
202
DATABASE
212
WATCHLISTS
240
INSTRUMENTATION SYSTEM
213
ALERTS
201
USER INTERFACE MANAGER
214
REPORTS
230
INTERDICTION SYSTEM
DB 231
215
CATALOGS
216
SEARCH ENGINE

FIG.2

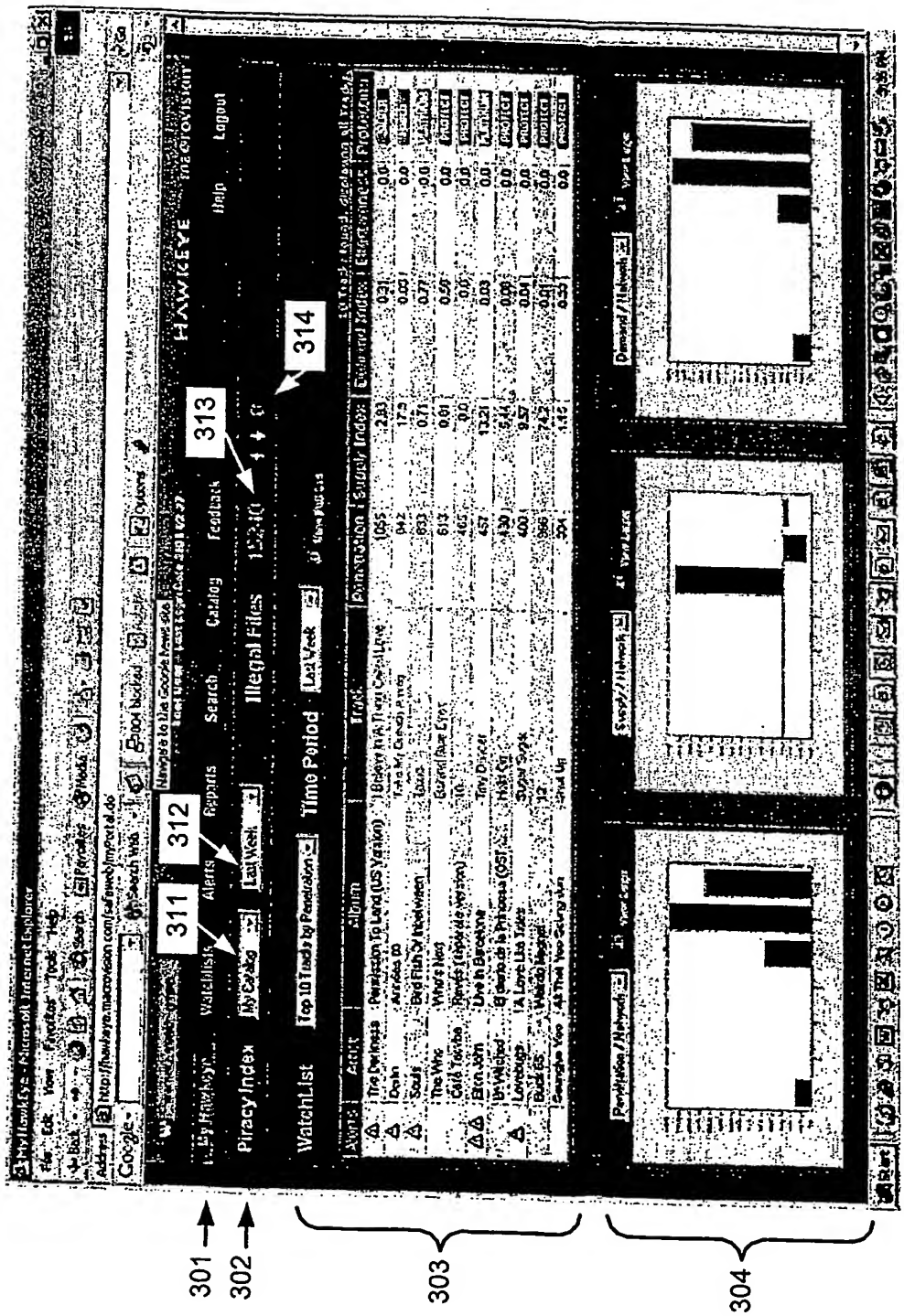

FIG.3

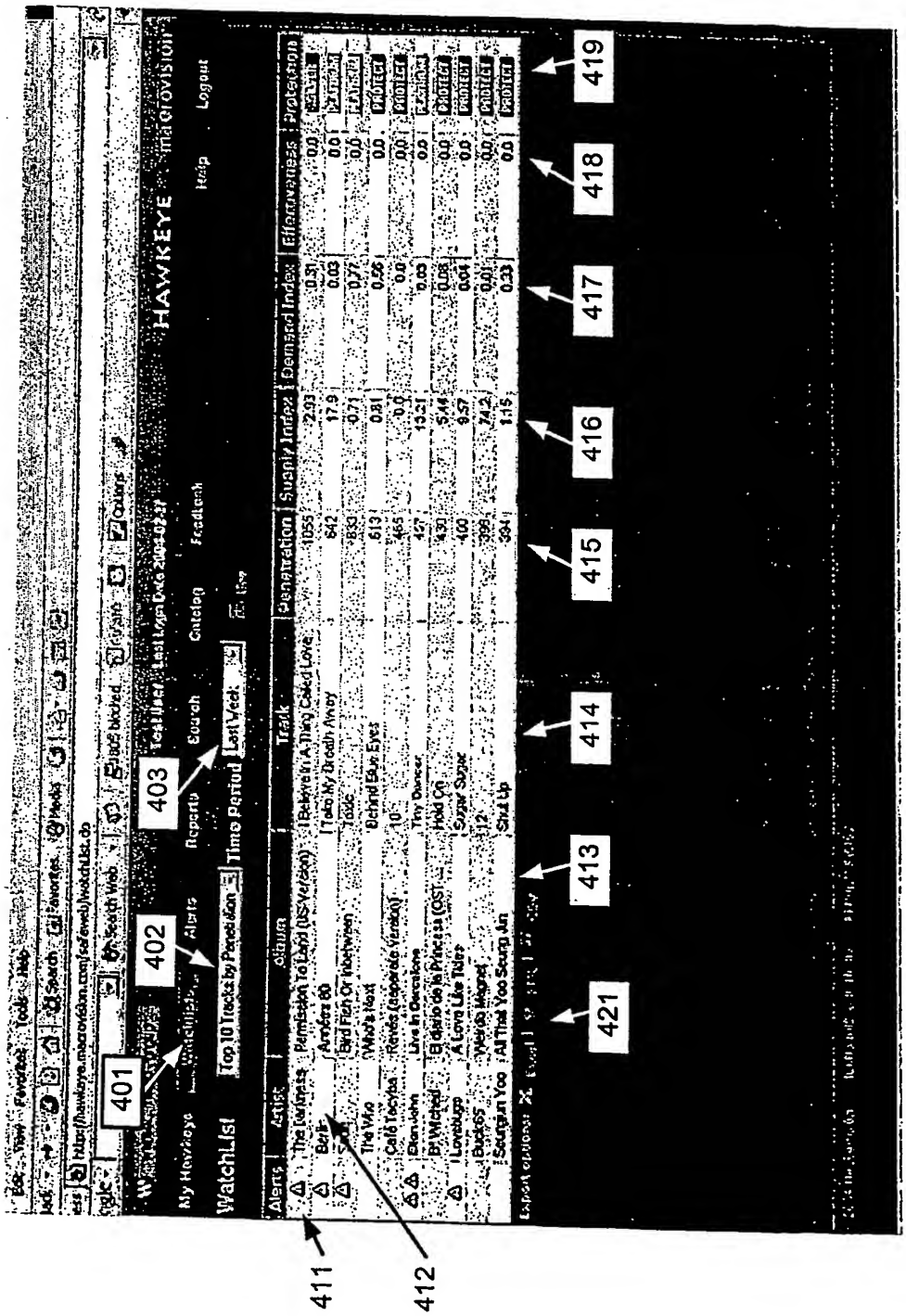
401
402
403
411
412
413
414
415
416
417
418
419
421
HAWKEYE
macrovision
Watchlist
Top 10 Tracks by Penetration
Last Week
Alerts
Artist
Album
Track
Penetration
Supply Index
Demand Index
Effectiveness
Protection

FIG.4

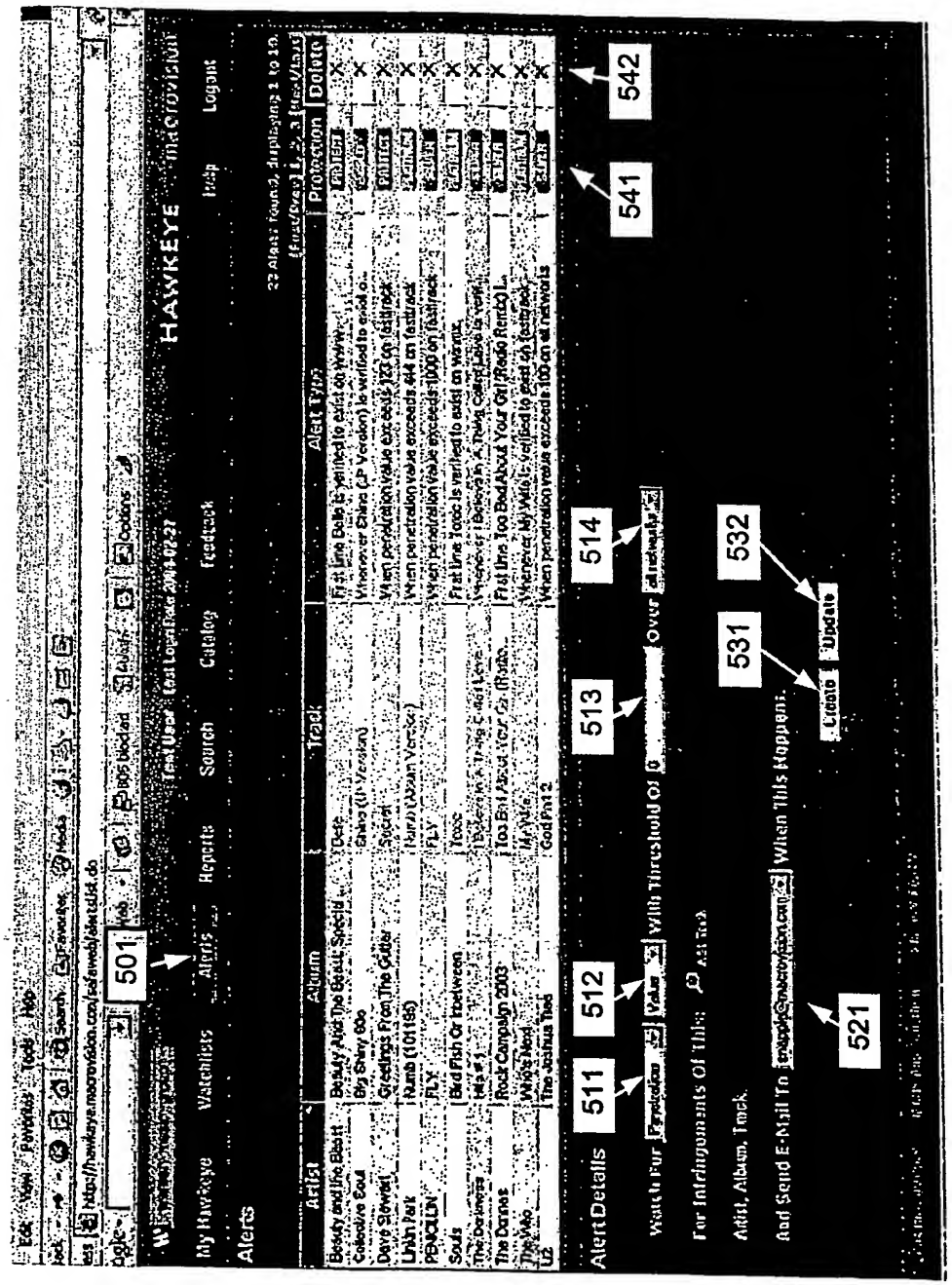
501
HAWKEYE
My HawkEye
Watchlists
Alerts
Reports
Search
Catalog
Feedback
Help
Logout
Alerts
Artist
Album
Track
Alert Type
Protection
Delete
Alert Details
511
512
513
514
521
531
532
541
542
Update

FIG.5

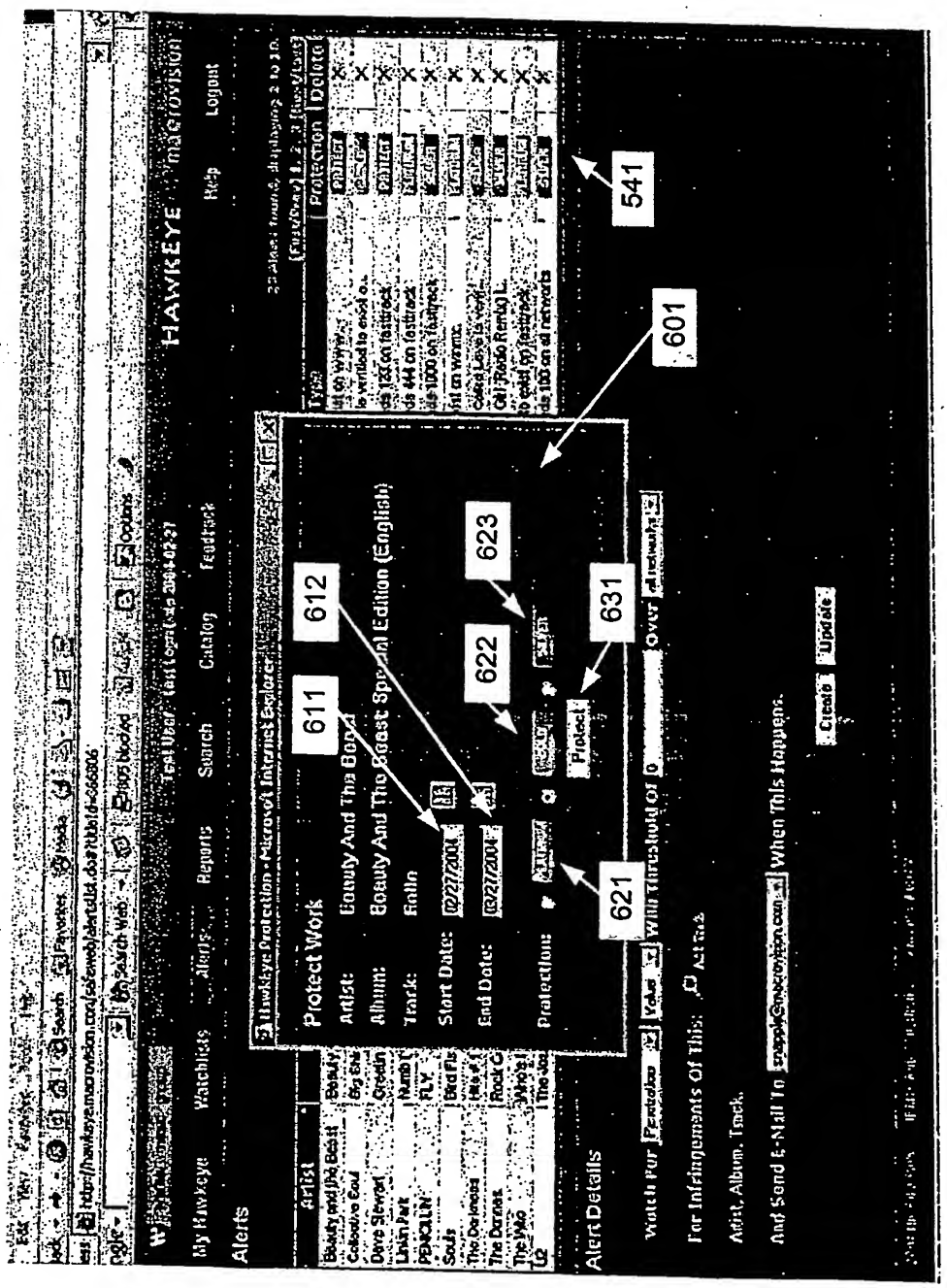
HAWKEYE
Protect Work
Artist:
Album:
Track:
Start Date:
End Date:
Protections:
Protect
Alert Details
Create
Update
611
612
621
622
623
631
601
541

FIG.6

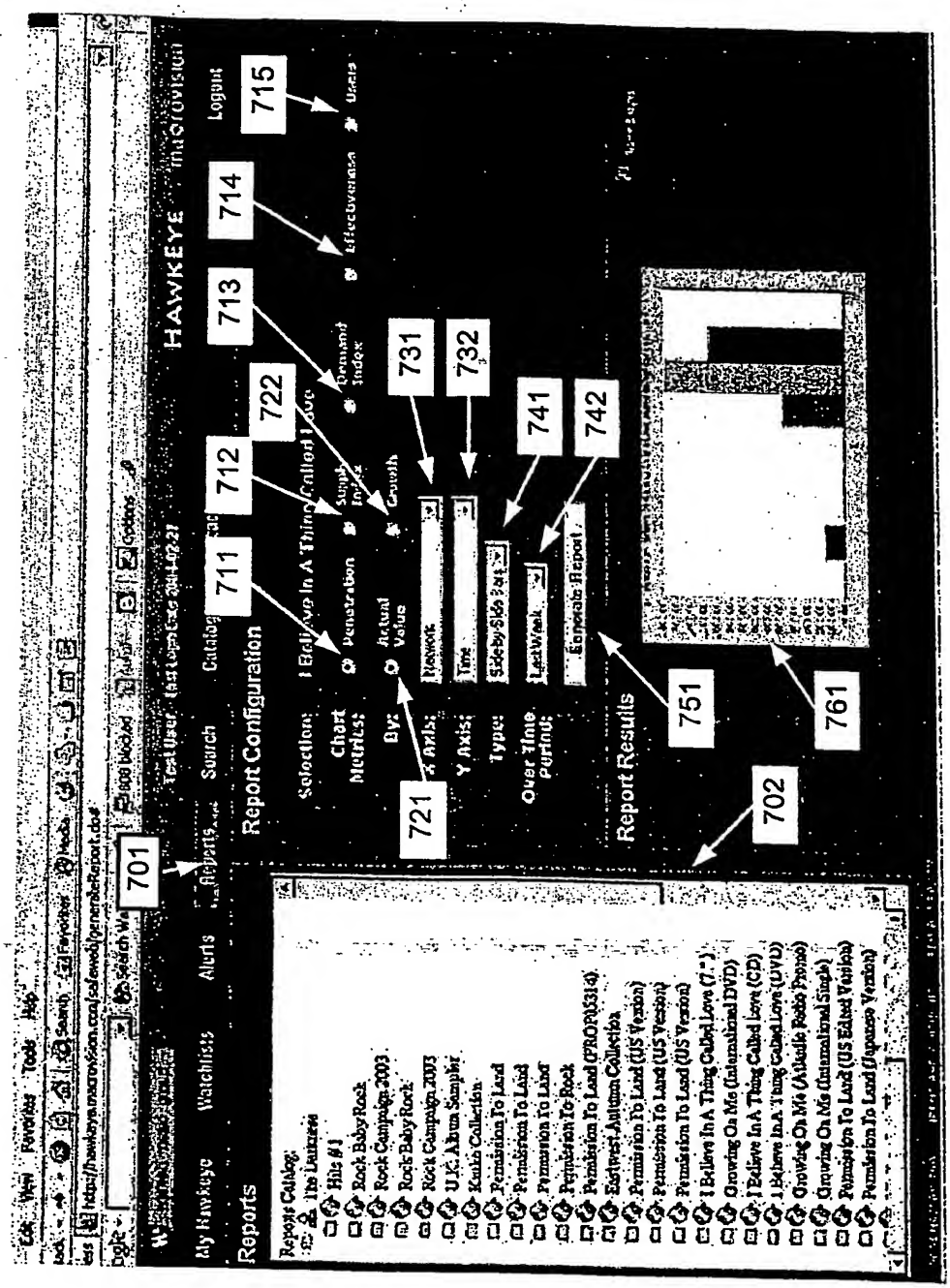
HAWKEYE
Logout
Reports
Report Configuration
Report Results
Selection:
Chart Metrics:
By:
X Axis:
Y Axis:
Type:
Over Time Period:
Generate Report
701
702
711
712
713
714
715
721
722
731
732
741
742
751
761

FIG.7

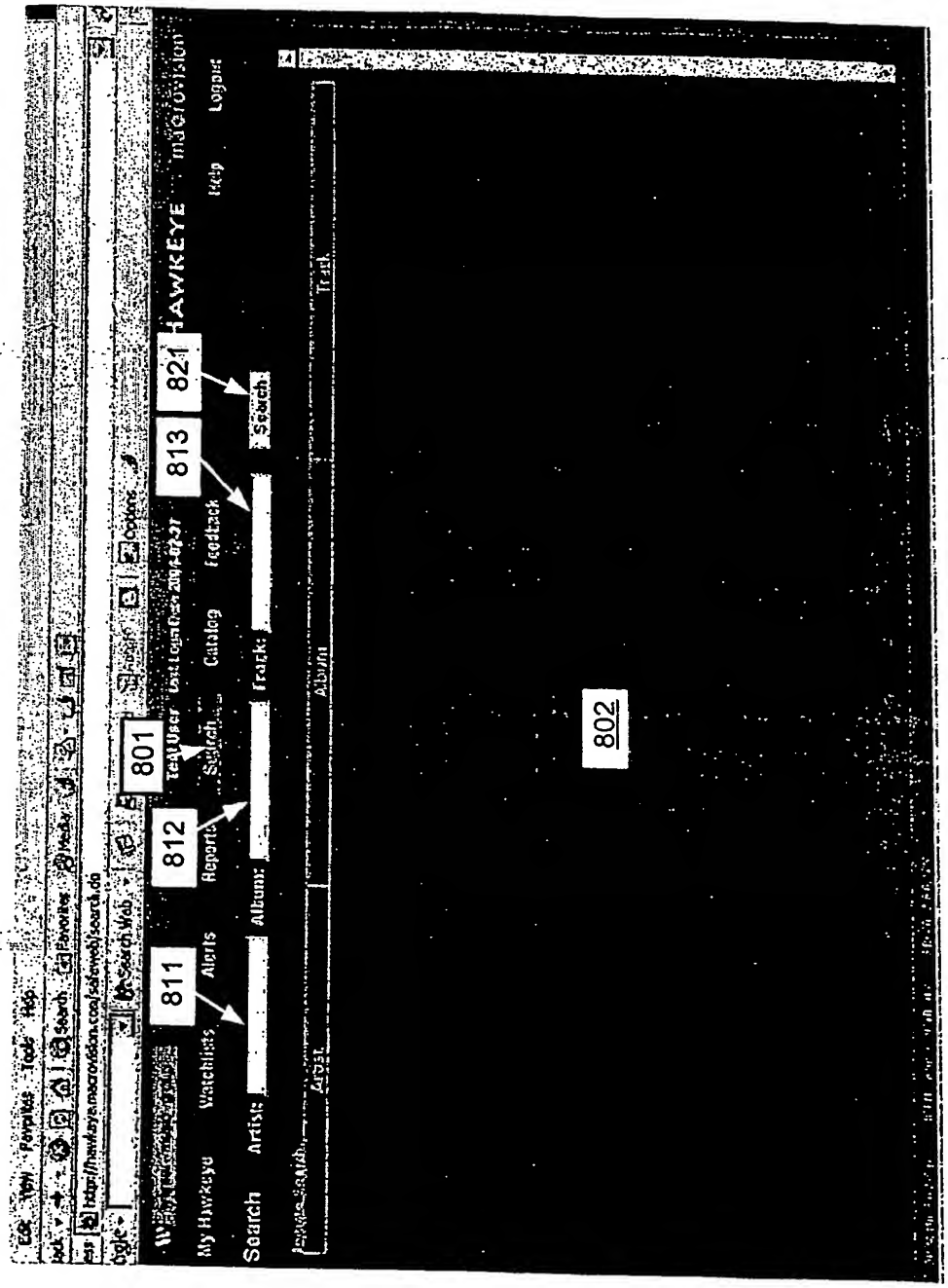
HAWKEYE
Search
Artist:
Albums:
Tracks:
Feedback
Search
801
802
811
812
813
821

FIG.8

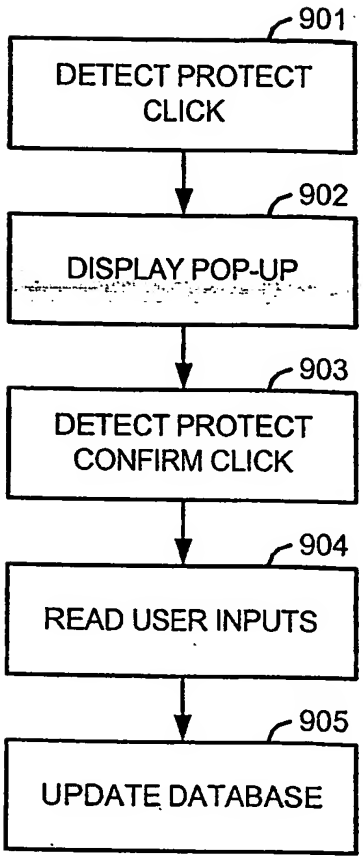
901
DETECT PROTECT CLICK
902
DISPLAY POP-UP
903
DETECT PROTECT CONFIRM CLICK
904
READ USER INPUTS
905
UPDATE DATABASE

FIG.9

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.